MẠNG KHÔNG DÂY RẤT DỄ BỊ BẺ KHOÁ

Hãng bảo mật McAfee cảnh báo các hệ thống mạng không dây rất dễ bị tin tặc đột nhập tấn công cho dù tính năng mã hoá có được kích hoạt đi chăng nữa. Foundstone - một đơn vị trực thuộc McAfee - khuyến cáo các công cụ bẻ khoá mã ho&aacut

Hãng bảo mật McAfee cảnh báo các hệ thống mạng không dây rất dễ bị tin tặc đột nhập tấn công cho dù tính năng mã hoá có được kích hoạt đi chăng nữa. Foundstone - một đơn vị trực thuộc McAfee - khuyến cáo các công cụ bẻ khoá mã hoá WEP và WPA giúp tin tặc tổ chức các vụ tấn công vào mạng không dây rất dễ được tìm thấy trên Internet. Đặc biệt một số phiên bản hệ điều hành Linux đã được cấu hình từ trước để thực hiện những vụ tấn công như vậy. Kẻ tấn công không cần có nhiều kiến thức để bẻ khoá hệ thống mã hoá của mạng không dây. Chính vì thế mà có rất nhiều lỗ hổng tiềm tàng có thể bị tin tặc khai thác tấn công. Mã hoá WEP có thể bị tin tặc sử dụng để "lắng nghe" các gói thông tin trao đổi giữa các hệ thống trong mạng không dây. Khi một số lượng các gói thông tin cần được thu thập, nó sẽ trở thành công cụ để bẻ khoá mã hoá và ăn cắp mật khẩu đăng nhập mạng không dây. Trong khi đó, WPA lại bị lợi dụng để đưa thêm các gói thông tin vào trong giao thông mạng khi một hệ thống thành phần của mạng tiến hành đăng nhập mạng - quá trình bắt tay tạo kết nối. Foundstone nhấn mạnh đến việc cần phải sử dụng một mật khẩu mạnh để tránh bị phát hiện đồng thời thay đổi mã khoá mạng thường xuyên. Foundstone cho biết hiện vẫn có 10% người dùng sử dụng một trong 50 mật khẩu thông dụng nhất. Martin Pivetta - giám đốc quản lý phát triển của McAfee - cho biết việc hãng quyết định công bố vấn đề bảo mật nói trên là muốn tạo ra ý thức bảo mật trong cộng đồng người dùng. Hoàng Dũng